Claims

What is claimed is:

[c1] A method of preventing unauthorized access to a computer system, comprising:

receiving a data packet at a firewall;

copying the data packet at the firewall;

analyzing the data packet with the firewall to determine if the data packet is authorized to access the computer system;

sending an authorized data packet to the computer system; and

denying access of an unauthorized data packet to the computer system.

[c2] The method of claim 1, further comprising:

dropping the unauthorized data packet.

[c3] The method of claim 1, further comprising:

logging the attempted access to the computer system of the unauthorized data packet.

[c4] The method of claim 1, wherein the computer system is a network.

[c5] The method of claim 1, wherein the data packet is analyzed by a pattern matching system.

[c6] A method of preventing unauthorized access to a computer system, comprising:

step of receiving data;

step of passively copying the data;

step of analyzing the data for authorization to access the computer system; and

step of allowing access to the computer system for authorized data; and

step of denying access to the computer system for unauthorized data.

[c7] The method of claim 6, further comprising:

step of dropping unauthorized data.

[c8] The method of claim 6, further comprising:

step of logging an attempt to access the computer system by unauthorized data.

[c9] A method of remotely managing a firewall, comprising:

receiving a control data packet at the firewall from a remote location;

copying the control data packet at the firewall;

analyzing the control data packet to determine if the control data packet is authorized to access the firewall; and

allowing an authorized control data packet to control the firewall.

[c10] The method of claim 9, further comprising:

dropping the authorized control data packet.

[c11] The method of claim 9, wherein the control data packet is analyzed for a password.

[c12] The method of claim 9, wherein the control data packet contains a false origination address.

[c13] The method of claim 9, wherein the control data packet contains a destination address that is protected by the firewall.

[c14] A method of remotely managing a firewall, comprising:

step of receiving control data at the firewall from a remote location;

step of copying the control data;

step of analyzing the control data to determine if the control data is

authorized to access the firewall; and

step of allowing authorized control data to access the firewall.

[c15] The method of claim 14, further comprising:

step of dropping the authorized control data.